



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/608,767

06/23/2003

Frank N. Adelstein

1032-007US01

8158

28863 7590 12/06/2007  
SHUMAKER & SIEFFERT, P. A.  
1625 RADIO DRIVE  
SUITE 300  
WOODBURY, MN 55125

EXAMINER

PARTHASARATHY, PRAMILA

ART UNIT

PAPER NUMBER

2136

NOTIFICATION DATE

DELIVERY MODE

12/06/2007

ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@ssiplaw.com

## Office Action Summary

Application No.

10/608,767

Applicant(s)

ADELSTEIN ET AL.

Examiner

Pramila Parthasarathy

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 26 September 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-122 is/are pending in the application.
- 4a) Of the above claim(s) 78-109 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-77 and 110-122 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date 10/27/2003.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_.

### **DETAILED ACTION**

1. This action is in response to the communication 09/26/2007. Claims 1 – 122 are currently pending.

#### ***Election/Restrictions***

2. Claims 78-86, 87-101 and 102-109 are withdrawn from further consideration pursuant to 37 CFR 1.142(b), as being drawn to a nonelected invention, there being no allowable generic or linking claim. Applicant timely traversed the restriction (election) requirement in the reply filed on 9/26/2007.

#### ***Information Disclosure Statement***

3. An initialed and dated copy of Applicant's IDS form 1449 is attached to the Office action.

#### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1 – 42, 43 – 70, 71-77, 110-112 and 113 – 122 are rejected under 35 U.S.C. 102(e) as being anticipated by Garza (US publication 2003/0208689).

5. As per Claims 1 and 113, Garza teaches "receiving input from a remote user of a client device that identifies computer evidence to acquire from a target computing device; acquiring the computer evidence from the target computing device with a forensic device coupled to the target computing device via a communication link; storing the computer evidence on the forensic device; and presenting a user interface for the forensic device through which the remote user views and analyzes the computer evidence acquired from the target computing device" (Fig. 1; paragraph [0010-0015 and 0020-0027]).

6. As per Claim 43, Garza teaches "a target computing device; a forensic device coupled to the target computing device via a communication link; a client device; and a user interface module to present a user interface for the forensic device that is remotely accessible by the client device, wherein the forensic device receives input via the user interface that identifies computer evidence to acquire from a target computing device and, in response, acquires the computer evidence from the target computing device, stores the computer evidence, and presents the computer evidence to the remote user for analysis via the user interface" (Fig. 1; paragraph [0010-0015 and 0020-0027]).

7. As per Claim 71, Garza teaches "receiving input from a remote user that identifies computer evidence to be acquired from a target computing device; determining an order in which to perform acquisition operations to acquire the computer evidence from the target computing device with reduced impact on other data stored on the target computing device, wherein acquisition operations to acquire at least one of a log file and communication statistics occur in the order prior to any other acquisition

operations; and communicating commands to initiate the acquisition operations on the target computing device in accordance with the determined order" (Fig. 1; paragraph [0010-0015 and 0020-0027]).

8. As per Claim 110, Garza teaches "A forensic analysis device that is adapted to operate as an intermediate device between a target computing device and a client device associated with a remote forensic investigator, wherein the analysis device comprises an acquisition module to acquire state information from the target computing device and store the state information on the forensic device while the target device remains active" (Fig. 1; paragraph [0010-0015 and 0020-0027]).

9. As per Claims 2, 44 and 114, Garza teaches "wherein presenting the user interface for the forensic device through which the remote user views and analyzes the computer evidence acquired from the target computing device comprises presenting the user interface for the forensic device through which the remote user views and analyzes the computer evidence acquired from the target computing device on-line" (paragraph [0010-0015]).

10. As per Claims 3-9, 12-19, 25, 45-49, 76-77, 111-112 and 115-118, Garza teaches "acquiring additional computer evidence while the remote user views and analyzes the previously acquired computer evidence" and "wherein receiving input from the remote user that identifies computer evidence to acquire comprises receiving input from the remote user that identifies at least one acquisition operation to perform, and further wherein acquiring the computer evidence from the target computing device comprises

performing the acquisition operation to acquire the computer evidence" (paragraph [0010-0015 and 0020-0027]).

**11.** As per Claims 10,11, 50,119-120, Garza teaches "automatically selecting at least one of a plurality of access methods via which to perform the acquisition operation based on the target computing device and the type of computer evidence to acquire; and communicating commands associated with the acquisition operation to the target computing device via the selected acquisition methods" and "wherein the access methods include at least one of Windows Management Instrumentation (WMI), Server Message Block (SMB), Secure Shell (SSH), Remote Shell (RSH), Network File System (NFS), Apple Filing Protocol (AFP), File Transfer Protocol (FTP), and Hypertext Transfer Protocol (HTTP)" (paragraph [0040-0058]).

**12.** As per Claims 20-21, Garza teaches "receiving authentication information from the user to verify the identity of the user, wherein the authentication information comprises one of a digital certificate or a username and password" (paragraph [0027]).

**13.** As per Claims 22-24 and 51-57, Garza teaches "receiving case information and target device information from a user to define a new inquiry; creating a new inquiry based on the received information; and associating the new inquiry with a case, wherein the target computing device information includes at least one of a target computing device host name, IP address, operating system, access methods and password" (paragraph [0027 and 0039-0040]).

Art Unit: 2136

**14.** As per Claims 26-27, 58-59, 60 and 121-122, Garza teaches "normalizing the acquired computer evidence to a common format; and storing the normalized computer evidence, wherein normalizing the acquired computer evidence to a common format comprises at least one of converting timestamp data from a local time zone of the target computing device to a standard time zone, converting data having host names and IP addresses to all host names, converting data having host names and IP addresses to all IP addresses, and normalizing the clock of the target computing device to that of the forensic device" (paragraph [0027 and 0039-0040]).

**15.** As per Claims 28 and 60, Garza teaches "performing a cryptographic hash on the computer evidence; and storing the resulting hash value" (paragraph [0030]).

**16.** As per Claims 29-30 and 61, Garza teaches "maintaining an audit log of transactions performed by the forensic device, wherein maintaining the audit log comprises at least one of tracking computer evidence downloaded from the target computing device, browsing of the computer evidence by the remote user, and analyses performed on the computer evidence, and wherein the audit log comprises a timestamp corresponding to each transaction, an investigator identifier corresponding to the investigator performing each transaction, and a description of each transaction" (paragraph [0032 and 0042-0059]).

**17.** As per Claims 31-38 and 62-66, Garza teaches "wherein the computer evidence comprises at least one log file, the method further comprising: receiving input from the user to analyze the log file for tampering; analyzing the log file to detect log file tampering; and displaying to the user the results of the analysis, wherein detecting

absent periodic events within the log file comprises: searching for the log file for the periodic event identifier; computing the amount of time that elapsed between each of the periodic event identifiers; and comparing the period of the event with the computed elapsed times to detect absent periodic events" (paragraph [0032 and 0042-0059]).

**18.** As per Claims 39 and 67 Garza teaches "wherein acquiring the computer evidence from the target computing device comprises acquiring an image of at least one of a disk attached to the target computing device and a memory of the target computing device, and further comprising examining the acquired image to identify at least one of files, process or operating system data structures, boot information, deleted files or directories, and data hidden in unallocated space" (paragraph [0035-0039 and 0042-0059]).

**19.** As per Claims 40-42 and 68-70 Garza teaches "wherein the target computing device comprises one of a personal computer, a handheld computer, a laptop, a workstation, a router, a gateway device, a firewall device, a web server, a file server, a database server, a mail server, a print server, a network-enabled personal digital assistant, and a network-enabled phone" (paragraph [0053-0061]).

**20.** As per Claims 72-75, Garza teaches "wherein communicating commands associated with the acquisition operations to the target computing device comprises: communicating commands associated with an acquisition operation to acquire communication statistics to the target computing device; communicating commands associated with an acquisition operation to acquire log file to the target computing device after the commands associated with the acquisition operation to acquire the



communication statistics, further comprising communicating commands associated with an acquisition operation to acquire general system information to the target computing device after the commands associated with the acquisition operation to acquire the log file" (paragraph [0053-0061]).

### ***Conclusion***

**21.** Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant.

Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

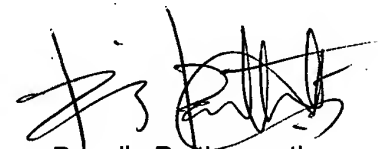
**22.** The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

Art Unit: 2136

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-232-4195. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Pramila Parthasarathy  
Patent Examiner  
Art Unit 2136  
December 02, 2007